Foreign National Cyber Access
Risk Assessment
Version 1.5
February 6, 2002

Division: APS Number: FNCA-APS1
Prepared by: W. P. McDowell Date: October 26, 2002
Service/Computer/Cluster: Desktop System PC/unix/Linux/Mac Argonne Employees

Instructions:

1. Use the form below to assess the vulnerabilities of your environment. Please extend the form if your environment has features not discussed below.
2. Identify the access controls you have in place to manage the user's environment. In addition to the standard login authentication processes, consider default file permissions, WWW content access, ftp server access, file sharing, etc. Provide enough detail to explain your answer.
3. Answering Yes or No to a question does not disqualify a legitimate user from accessing a computer system. Rather these questions are designed to help you assess the risks involved in granting any user access to a computer system by highlighting potential concerns.
4. You should only need one of these vulnerability assessments for each computing environment. Please update this form if your environment changes significantly.
5. Keep this on file in your division.

If this user will be provided a computer:

	Vulnerabilities	Response/Access Controls
1.	Are there data or applications on the computer that this user will be using that are on the ANL Sensitive Technologies List or otherwise sensitive (privacy act, proprietary, OUO, etc.)?	No.
2	Describe the mechanisms that will prevent this user from examining, altering, or using inappropriate applications or data on his computer? For example	Unnecessary. See 1.
2.1	Have you removed the inappropriate data or applications?	No. See 1.
2.2	Are all users instructed in the secure management of data and applications?	Yes. All users take the annual ESH 223 computer protection training.
2.3	Does the computer system require authenticated access?	Yes.
2.4	Can you uniquely identify users?	Yes.
2.5	Do you establish minimal default file permissions for all accounts?	Yes.
2.6	How do you verify file permissions are correctly set for data and applications?	Scans and Audits.

If this user will be provided network access to computer services (mail, ftp, etc.):

	Vulnerabilities	Response/Access Controls
3.	Are there data or applications on the servers that this user will access that are on the ANL Sensitive Technologies List or otherwise sensitive (privacy act, proprietary, OUO, etc.)?	No.
4.	Describe the mechanisms that will prevent this user from examining, altering, or using inappropriate applications or data stored on computers providing these services? For example:	Only System Administrators are allowed to log in to the Servers File servers: Users on login This authenticates files share on the file server. Account setup enables users to only access their share.

		Mail servers: Users authenticate to our mail server. This authentication limits users to their specific mailboxes on the server.
4.1	Does having access to this server enable unauthenticated access to a local intranet (by virtue of having an *division.anl.gov* address)?	No. These servers do not permit subsequent connection to other services.
4.2	Does having an account on this server enable authenticated access to other computers?	No. See 4.1
4.3	Are other computers sharing file systems that may be accessible from this server (e.g. NFS, Windows file shares)?	No. See 4.1
4.3.1	If yes, how do you control network file access?	
4.3.2	How do you verify network file permissions are correct?	

If this user's network connection provides intimate[1] access to a computing environment:

	Vulnerabilities	Response/Access Controls
5.	Are there data or applications in the network vicinity of this user's computer that are on the ANL Sensitive Technologies List or otherwise sensitive (privacy act, proprietary, OUO, etc.)?	Possibly,. this network does permit hosts on this network to electronically reach other ANL hosts which may have sensitive data.
6.	Describe the mechanisms that will prevent this user from examining, altering, or using inappropriate applications or data stored on computers in the vicinity? For example (consider using nmap on the subnet to identify open services):	The APS servers require authenticated access. The division subnet is a switched media. A malicious user cannot use a network sniffer to collect packets.
6.1	Does having access to this computer enable unauthenticated access to a local intranet (by virtue of having an *division.anl.gov* address)?	Yes. Our division operates a WWW server for division personnel that provides procedures for administrative tasks. Access to the local network permits access to the ANL intranet.
6.2	Does having an account on this computer enable authenticated access to other computers?	No..
6.3	Are other computers sharing file systems that may be accessible to this computer (e.g. NFS, Windows file shares)?	No. Unrestricted file shares are not permitted at the APS.
6.3.1	If yes, how do you control network file access?	Login authication
6.3.2	How do you verify network file permissions are correct?	Periodic scans and internal audits.

[1] For example: What is visible in the Network Neighborhood? Are there unrestricted NFS exports on the local network? If a user runs tcpdump or places an ethernet interface in promiscuous mode, what will they see?